ABSTRACT

A multiplication module, including a first input unit and a second input unit, for multiplying m bits of data in a Galois field $GF(2^m)(m \geq 1)$, includes: first and second power arithmetic units for receiving the first m bits of data from the first input unit; a first multiplication unit for receiving the first m bits of data and the output of the first power arithmetic unit; a second multiplication unit for receiving second m bits of data from the second input unit and the output of the second power arithmetic unit; a selection unit for receiving an output signal from the second multiplication unit and the second m bits of data; and a control unit for outputting a control signal to the first power arithmetic unit, the second arithmetic unit and the selection unit, wherein the first power arithmetic unit receives a first control signal, the second power arithmetic unit receives a second control signal, and the selection unit receives a third control signal, for controlling the output of the selection unit, while the first multiplication unit outputs a first output signal, and the selection unit outputs a second output signal.